Abstract

A method and apparatus enhancing the security of an encrypted cryptographic key by storing its key re-transforming information in a decryption store that is separate from a cryptographic key store, which stores the encrypted cryptographic key, from which accessing circuitry is able to access the encrypted cryptographic key. The cryptographic key store may be a disk drive of a computer, the decryption store may be a network access card installed in that computer or a mobile terminal coupled to that computer, and the accessing circuitry may be the computer's controller. Decryption of the encrypted cryptographic key is carried out in the decryption store, as is the subsequent encryption or decryption using the decrypted cryptographic key. The accessing circuitry communicates with the decryption store exclusively via a predetermined interface, where the interface does not allow the accessing circuitry access to the cryptographic key and to at least a portion of the key re-transforming information from the decryption store. Thus, the encrypted cryptographic key can be stored relatively insecurely; while the security of the cryptographic key is maintained at a very high level because there is no native capability for the computer to randomly read information from the network access card or the mobile terminal.